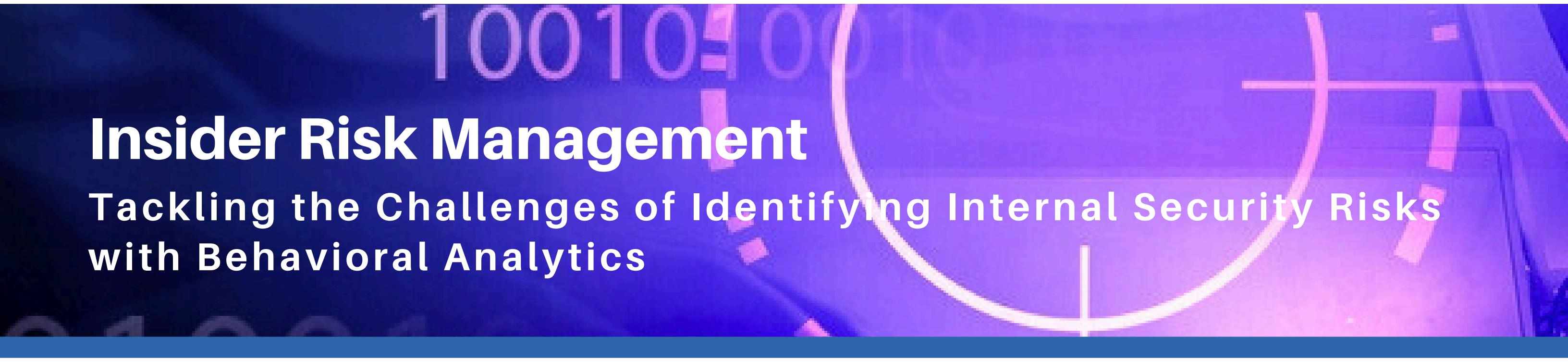

Insider Risk Management

Tackling the Challenges of Identifying Internal Security Risks with Behavioral Analytics

THE PROBLEM

Organizations face growing challenges in safeguarding sensitive data and systems from insider risks. These risks arise from trusted insiders—employees, contractors, or other internal stakeholders—who may intentionally or unintentionally expose an organization to harm. Addressing insider risk requires a nuanced understanding of insider behaviors, as traditional security tools primarily focus on external threats and often fail to detect threats from within acceptable permission boundaries.

Insider risk can be categorized into three primary types:

- **Negligent Insiders** - Not all suspicious activity is actually malicious. Negligence arises from unintentional mistakes due to lack of training, awareness, or safeguards.
- **Malicious Insiders** - Insiders who deliberately exploit their trusted access to harm the organization for personal, financial, or ideological gain.
- **Compromised Insiders** - Insiders whose access or credentials are hijacked by external actors, turning them into proxies for malicious activities. These incidents often appear legitimate but are conducted with malicious intent.

OUR SOLUTION

Applying Contextual Behavioral Analytics to Mitigate Challenges

Unlike traditional security tools that focus on detecting external threats through log analysis, WireX Systems Ne2ition Platform uses contextual behavioral analytics to track and analyze detailed user activities in real-time. By monitoring patterns of access, including what data is accessed, when it is accessed, and how it is accessed (including detailed query analysis), WireX Systems can detect anomalous activities that would otherwise go unnoticed.

WireX Systems provides deep insight into data interactions and user behaviors beyond simple login attempts, giving security teams the context they need to identify potential insider threats, even when actions appear routine or gradual. With real-time threat detection, data set discovery, and rapid incident response capabilities, WireX Systems helps organizations mitigate risks before they escalate, ensuring they can act quickly to protect sensitive data while maintaining compliance.

1. **Real-Time Visibility**
   Comprehensive monitoring of user activities across cloud and on-premise environments.
2. **Behavioral Analytics**
   Track and analyze user behavior patterns, identifying anomalies in how data is accessed and used.
3. **Context-Aware Monitoring**
   Detect gradual or non-obvious malicious behaviors that blend into routine activities.
4. **Proactive Risk Mitigation**
   Identify vulnerabilities and unusual behavior early, reducing potential security gaps.
5. **Enhanced Compliance Efforts**
   Comprehensive visibility into data flows and user actions across all environments.

© 2025 All rights reserved.